AFFIDAVIT OF SPECIAL AGENT MICHAEL LIVINGOOD IN SUPPORT OF AN APPLICATION FOR A COMPLAINT AND SEARCH WARRANT FOR EMAIL ACCOUNT

I, MICHAEL LIVINGOOD, state:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since June 2016. I am assigned to the Economic Crimes Squad in the FBI's Boston, Massachusetts Field Office. My duties include investigating money laundering, wire fraud, and internet fraud. I have participated in the execution of warrants involving the search and seizure of computers, computer equipment, and electronically stored information. Before becoming a Special Agent, I was an Intelligence Analyst for the FBI and supported investigative work on a variety of federal crimes including crimes against children, transnational organized crime, and money laundering. I have received specialized training in investigating financial frauds and money laundering. I hold a master's degree in human services. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

2. This affidavit is being submitted in support of an application for:

   (a) a criminal complaint charging Nosayamen Iyalekhue (Iyalekhue) and Esogie Osawaru (Osawaru) with violations of 18 U.S.C. § 1343 (Wire Fraud), and

   (b) an application for a warrant under 18 U.S.C. § 2703(a) and Rule 41 of the Federal Rules of criminal Procedure to search and seize records and data from the e-mail account identified as jennyrbts11@outlook.com (the Target Email Account") as described in Attachment A, because there is probable cause to believe that it contains evidence, fruits and instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy), 1028 (Identification Fraud), 1030 (Computer Fraud), 1343 (Wire Fraud), 1344 (Bank Fraud), 1546 (Passport Fraud), 1956 (Money Laundering), and 1957 (Unlawful Monetary Transactions), as described in Attachment B.

3. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested search warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE THAT CRIMES WERE COMMITTED

4. As set forth below, there is probable cause to believe the following: from on or about 2016 through the present, Nosayamen Iyalekhue, Esogie Osawaru, and others participated in a series of romance, pandemic unemployment insurance, and other on-line scams designed to defraud victims into sending money to accounts controlled by them in their own names and under other names used by them. To carry out the scams, they used false foreign passports, in the names of others but with their photos, to open numerous bank accounts, and in turn directed the victims to send the victims' money to these accounts. Iyalekhue and Osawaru, and potentially others known and unknown, then rapidly withdrew the victims' money from various bank branches and ATM's, often multiple times on a single day. As set forth below, Iyalekhue and Osawaru used accounts in the names of Mathew Lungelo, Jude Ekanem, Howard Bhekani, Franklin Edward and Anthony Milk, among others, to receive and withdraw victims' funds.

5. Based on the e-mail address's domain name, I have probable cause to believe that the Target Email Account and relevant data are maintained by Microsoft Corporation ("Microsoft"), which, government databases indicate, accepts service of process at:

1 Microsoft Way, Redmond, WA 98052 via Web Portal
USLEReq@Microsoft.com as described in Attachment A.

I. Nosayamen Iyalekhue

A. Iyalekhue Used Position as Bank Teller to Access Accounts in Other Names.

6. According to records of TD Bank and reports from TD Bank investigators, Iyalekhue was employed as a teller at the TD Bank located at 143 Nahatan Street, Norwood, Massachusetts, 02062 between August 13, 2018 and August 12, 2019.

7. In July 2019, TD Global Security and Investigation became aware that Iyalekhue had been accessing customer accounts at times when no customer was present, which violated bank policy. In particular, TD Bank determined from its records that Iyalekhue accessed accounts in the name of "Jude Ekanem," "Milk Anthony," "Franklin Edward," and others. TD Bank subsequently terminated Iyalekhue's employment at TD Bank due to his conduct.

B. Iyalekhue Created Accounts in the Names of Others To Receive Victim Funds

Accounts in the Name of Mathew Lungelo at Santander, Bank of America, and Eastern Bank

8. Records from Santander Bank, Bank of America, and Eastern Bank show accounts opened in the name of Mathew Lungelo using a Liberian passport. The photo on the Mathew Lungelo passport, however, appears to be Iyalekhue. For example, Figure 1.1 below is copy of the passport provided to Santander at the time the Lungelo account was opened. Figure 1.2 is a copy of Iyalekhue's Massachusetts Driver's License photo. Photos of what appear to be the same passport were also found in the records of the opening for the Lungelo accounts at Eastern Bank in the name of Mathew Lungelo.

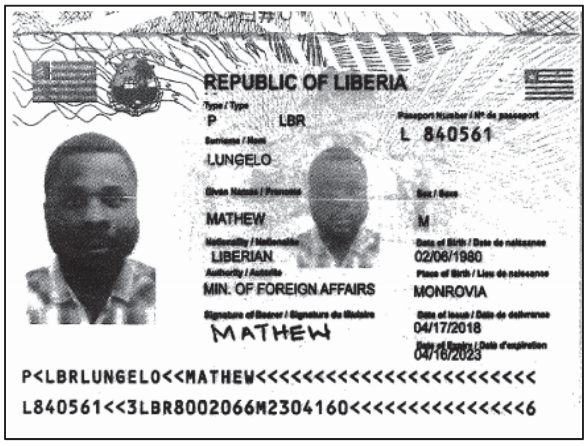

Fig. 1.1 Mathew Lungelo Liberian Passport Provided to Santander Bank

Fig. 1.2 Iyalekhue Massachusetts Driver's License Photo

9. In each account application, the person purporting to be Mathew Lungelo also claimed not to be a U.S. citizen. I have searched United States Department of Homeland Security ("DHS") records and was unable to locate travel or Visa records for this passport, which lists all entries by foreign citizens.

10. The Santander account ending in 1157 (the Santander Lungelo account) was opened on or about October 15, 2019. The Bank of America account ending in 2816 (the Bank of America Lungelo account) on or about October 15, 2019. The Eastern Bank account ending in 4974 (the Eastern Lungelo Account) was opened on or about February 20, 2020. All three accounts were opened at branches in Massachusetts. For each account, Lungelo was the sole authorized account signatory on the account. The address 49 Dana Ave., #2, Hyde Park, MA, was used for each account at the time of opening. Moreover, the email address provided for each account at the time of opening was the Target Email Account (jennyrbts11@outlook.com).

Accounts in the Name of Jude Ekanem at TD Bank, Bank of America, and Santander

11. As noted above, while working at TD Bank, Iyalekhue accessed the Ekanem TD Bank account. Records from TD Bank, Bank of America, and Santander Bank for accounts in the name of "Jude Ekanem" also show the following:

12. On August 19, 2017, a person purporting to be Ekanem opened an account ending in 2284 (the Ekanem Santander account) at a branch in Massachusetts. Ekanem was the sole authorized account signatory on the account. The Target Email Account was also provided during account opening. A Ghanian passport was used to open the account and the applications indicated that Ekanem was not a United States citizen. I have searched DHS records and was unable to locate travel or Visa records for this passport. As with the Lungelo accounts, the identification used to open the Ekanem Santander account appears to be Iyalekhue. Figure 1.3 below is copy of the passport provided to Santander at the time the Ekanem account was opened.

Fig. 1.3 Jude Ekanem Ghanian Passport Provided to Santander Bank

13. On February 21, 2018, a person purporting to be Ekanem opened a TD Bank account ending in 0535 (the Ekanem TD Bank account) at a TD Bank branch in Massachusetts. Ekanem was the sole authorized account signatory on the account.

14. Bank of America records reflect that on or about August 19, 2017, a Bank of America account ending in 9968 (the Ekanem Bank of America Account) was opened at a branch in Massachusetts. At the time of account opening Ekanem provided the address 11

Wilcock St., Dorchester Center, MA. Ekanem was the sole authorized account signatory on the account. The Target Email Account was also provided during account opening.

Accounts in the Name of Howard Bhekani at Santander, Rockland, Bank of America, and Citizens

15. Bank records from Santander Bank, Rockland Trust, Bank of America, and Citizen's Bank show accounts held in the name of Howard Bhekani were also opened. The Target Email Account was also provided at the time the Bank of America and Santander Bhekani accounts were opened.

16. Santander Bank records show that on or about October 24, 2018, an account in the name of Howard Bhekani ending in 5621 (the Bhekani Santander account) was opened at a branch in Massachusetts. Bhekani was the sole authorized account signatory on the account. The account was opened using a South African passport. I have searched DHS records and was unable to locate travel or Visa records for this passport. Figure 1.4 below is copy of the passport provided to Santander at the time the Bhekani account was opened.

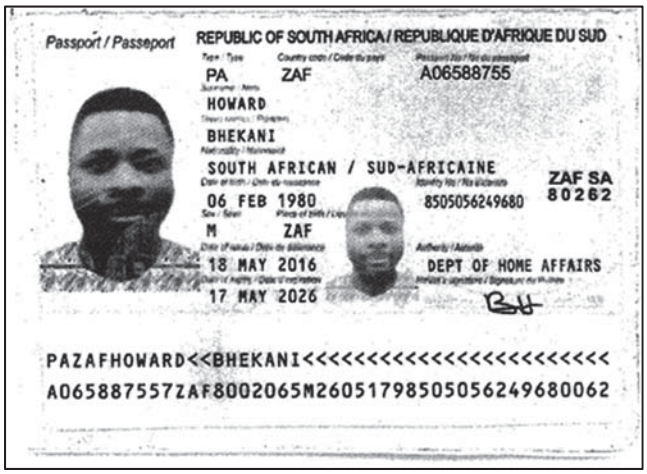

Fig. 1.4 Howard Bhekani South African Passport Provided to Santander Bank

The passport photo appears to be the same person as the photo of Iyalekhue above, as well as the passport photos for Mathew Lungelo and Jude Ekanem.

17. Bank records from Bank of America, Citizen's Bank, and Rockland Trust, also show that accounts were opened in Bhekani's name on October 24, 2018 (Bank of America Bhekani account ending in 2614), July 10, 2019 (Citizen's Bank Bhekani account ending in 3368), and May 15, 2019 (Rockland Trust Bhekani account ending in 1824). Bhekani was also the sole authorized account signatory on these accounts. For the Citizen's Bank Bhekani account and the Rockland Trust Bhekani account, the address 49 Dana Ave., #2, Hyde Park, MA, was provided during account opening. As noted above, this is also the address provided for the Lungelo accounts.

II. Esogie Osawaru

A. Osawaru Created Accounts in the Names of Others to Send and Receive Funds.

18. As noted above, two of the TD Bank accounts that Iyalekhue improperly accessed before he was terminated were accounts in the names of "Franklin Edward" and "Milk Anthony." According to TD Bank investigators, the holder of these two accounts appeared on bank surveillance to be the same person, based on appearance, clothing, and distinctive jewelry, in particular gold colored earrings in the shape of a cross.

Accounts in Name of Franklin Edward at TD Bank and Bank of America

19. Bank records from TD Bank and Bank of America show that in 2018, two accounts were opened at Massachusetts branches in the name of Franklin Edward - a TD Bank account ending in 7048 (the Edward TD account) and a Bank of America account ending in 9385 (the Edward BOA account). Both were opened with a United Kingdom passport in the name of Franklin Edward.

20. The applications for both accounts also indicated that Edwards is not a U.S. citizen. I have searched DHS records and was unable to locate travel or Visa records for this passport. Edward was the sole authorized account signatory on the account.

21. Edward's BOA account listed the address for Franklin Edward as address 11 Wilcock St., Dorchester Center, MA. This is also the same address used in connection with opening documents for Jude Ekahem described above.

22. As set forth below, bank surveillance of activity in the Edward TD Bank account (Figure 2.2) captures an individual who appears to be the same person as in the Massachusetts Department of Registry of Motor Vehicles driver's license for Osawaru (Figure 2.1), wearing the same gold colored earrings in the shape of a cross.

Fig. 2.1 Osawaru's Massachusetts Driver's License Photo

Fig. 2.2 TD Bank ATM Surveillance Image of Feb. 7, 2019 Withdrawal from Edward Account.

Accounts in Name of Milk Anthony at TD Bank, Citizen's Bank, and Santander Bank.

23. Bank records from TD Bank, Citizen's Bank, and Santander Bank also show three accounts in the name of Milk Anthony - a TD Bank account ending in 9224 (the Anthony TD account), a Citizen's Bank Account ending in 4264 (the Anthony Citizen's account), and a Santander Bank account ending in 1949 (the Anthony Santander account). Anthony was the sole

authorized account signatory on these accounts. All Anthony accounts were opened at bank branches in Massachusetts in 2019. Additionally, all three accounts were opened with a Nigerian passport in the name of Milk Anthony (A02308508). Below is copy of the passport provided to TD Bank, Citizen's Bank, and Santander Bank at the time the Anthony accounts were opened.

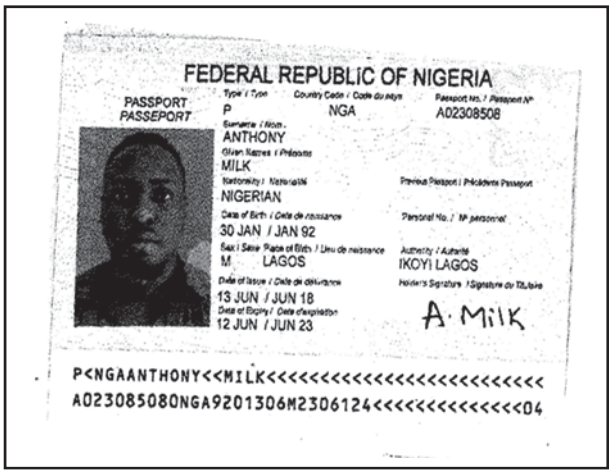

Fig. 2.3 Milk Anthony Nigerian Passport Provided to TD Bank, Citizen's Bank, and Santander Bank.

24. Also, as depicted in Figure 2.4, surveillance photos from these accounts also show a person who appears to be the same person as Osawaru and is wearing the gold colored earrings in the shape of a cross.

Fig. 2.4 TD Bank Surveillance Image of Mar. 30, 2019 from Anthony Account.

25. I have searched DHS records and located Visa application for this passport number; however, the passport was in a different name, was refused a Visa, and expired October 31, 2015.

26. At the time of the Anthony Santander and TD Bank accounts opening, the address 49 Dana Ave., #2, Hyde Park, MA, was provided. As described above, this is the same address used in the account opening documents for the Howard Bhekani, Mathew Lungelo, and Franklin Edward. Bank records from Santander Bank also show that Osawaru opened an account in his own name on October 9, 2018 using 49 Dana Ave. #2, Hyde Park, MA. .

III. Iyalekhue and Osawaru Used the Fake Bank Accounts to Receive Fraud Proceeds from Victims Throughout the Country.

A. Victim-1 from Florida Sends Funds to Iyalekhue's Lungelo Accounts.

27. On or about March 2, 2020, I interviewed Victim-1 from Clearwater, Florida, who reported that she had been a victim of an on-line fraud. Victim-1 was in the hospital in late 2019 due to a chronic medical condition, when she was contacted via email by someone that Victim-1 believed she had known in high school. The purported high school friend (CC-1) told Victim-1 that the he ran a very successful international company and needed to give away some of their profits. CC-1 offered Victim-1 a job helping to distribute funds for philanthropic purposes. Victim-1 was told she would be paid 5 percent of the funds that she distributed. Victim-1 believed this job offered a way to help people and make extra money.

28. Victim-1 received checks from CC-1, deposited them, and immediately sent wires to the bank accounts designated by CC-1, including the Bank of America and Santander accounts in the name of Matthew Lungelo.

29. The first checks deposited by Victim-1 returned as checks not on a valid account. Victim-1 confronted CC-1 via text message who told Victim-1 that CC-1 had set things up

incorrectly and asked Victim-1 to deposit additional checks. Victim-1 believed CC-1 and deposited more checks, which were also returned as not checks on a valid account. After this, Victim-1 deposited no further checks. Victim-1 reported that she deposited a total of approximately $240,000 in checks from this purported on-line friend, all of which returned as not checks on a valid account.

30. Because of this fraud scheme, Victim-1's account dropped into a negative balance. Victim-1 never earned any money, as CC-1 always told her she would be paid after doing more transactions.

31. Bank of America records also show that on December 10, 2019, Victim-1 wired $30,000 of the funds to the Lungelo Bank of America account ending in 2816. Between December 10 and December 16, 2019, six cash withdrawals totaling $11,900 were made from this Bank of America account at a branch in Massachusetts before Bank of America closed the account due to the alleged fraudulent activity. Video captured by Bank of America shows withdrawals being made by Iyalekhue. For example, Figure 3.1 is a still image taken from a Bank of America surveillance video on December 14, 2019 as $1,000 is withdrawn from the Lungelo account ending in 2816. The image depicts Iyalekhue making the withdrawal.

Fig. 3.1 Bank of America ATM Surveillance Image of Dec. 14, 2019 Withdrawal from Lungelo Account.

On December 6, 2019, Victim 1 sent a wire in amount of $22,475 to the Lungelo Santander Bank account ending in 1157. Between December 6, and December 9, 2019, $22,400 was withdrawn in five cash withdrawals from Santander branches in Massachusetts.

B. Victim-2 from Texas Sends Funds to Iyalekhue's Lungelo, Bhekani, and Ekanem Accounts.

32. On or about February 25, 2020, I interviewed Victim-2, from Panna Maria, Texas, who is 64 years old. Victim-2 told me she had been communicating with a man (CC-2), whom she had never met in person, for approximately 4 years. Victim-2 believed that CC-2 originally lived in the United States, but early in their communications CC-2 went to South Africa. Victim-2 believed CC-2 was in trouble and she had been sending him money to assist with legal fees and other personal needs.

33. Victim-2 stated that she sent money to Mathew Lungelo and Jude Ekanem at the direction of CC-2. In addition, Santander Bank account records show that Victim-2 also sent money to the Santander Bhekani account.

34. Santander Bank records show that Victim-2 made wire transfers to the Santander Lungelo account ending in 1157 on or about November 26, 2019 for $11,000 and on or about December 30, 2019, for $9,000. The funds were immediately depleted via cash withdrawals.

35. A Santander Bank representative reported that the bank attempted to contact the person purporting to be Lungelo regarding the account activities due to concerns that the account was being used to launder money. No one ever responded.

36. Records of Santander Bank and Bank of America show that on or about the dates listed below, Victim-2 sent the amounts listed below to the listed accounts. Victim-2 reported that she sent these amounts pursuant to the direction of CC-2.

Approximate Date	Amount	Receiving Account
9/29/2017	$9,500	Ekanem Santander
10/6/2017	$6,500	Ekanem Santander
10/26/2017	$9,000	Ekanem Santander
12/20/2017	$12,000	Ekanem Santander
01/30/2018	$15,000.00	Ekanem BOA
03/09/2018	$5,000.00	Ekanem BOA
02/23/2018	$16,000.00	Ekanem BOA
02/09/2018	$4,000.00	Ekanem BOA
11/26/2019	$11,000	Lungelo Santander
12/30/2019	$9,000	Lungelo Santander
11/30/3018	$9,000	Bhekani Santander
12/17/2018	$8,000	Bhekani Santander
12/27/2018	$4,500	Bhekani Santander
1/4/2019	$3,000	Bhekani Santander
1/28/2019	$4,000	Bhekani Santander

In each instance, these funds were depleted from the account into which they were deposited by cash withdrawals, usually within a few days of receipt of the funds.

C. Victim-3 from Michigan Sends Funds to Iyalekhue's Bhekani Account and Osawaru's Edward Account.

37. On February 20, 2020, I interviewed Victim-3 from Wyandotte, Michigan, who told me she had met a man (CC-3) while playing an online game in 2018. Victim-3 has never met CC-3 in person but over time developed a relationship over telephone and internet communication. Victim-3 believed CC-3 lived on an oilrig. CC-3 began requesting loans from Victim-3 for various purported needs. Victim-3 began sending money at CC-3's request.

38. Documents provided by Victim-3 show that she sent this money to Howard Bhekani and Franklin Edward. Victim-3 estimated she had sent over $100,000 at the direction of CC-3.

39. According to Santander Bank records, Victim-3 sent a $8,250 wire to the Bhekani Santander account ending in 5621 on December 11, 2018. These funds were quickly depleted by cash transactions directly following the deposit.

40. Between October 2018 and March 2019, Victim-3 attempted to send three wires from her account in Michigan totaling $82,900 to the Edward TD Bank account in Massachusetts ending in 7048 as follows:

Date	Amount	Method	Result
10/11/18	$30,600	Wire	Received by TD Bank in MA
11/26/2018	$24,800	Wire	Received by TD Bank in MA
3/11/2019	$27,800	Wire	Attempted but funds denied

41. The funds that were received were withdrawn via cash withdrawals at various TD Bank Massachusetts branches.

42. Around March 2019, TD Bank questioned the person purporting to be Edward about the wires and the large cash withdrawals. This person told TD Bank that he purchased cars and shipped them to various African countries.

43. Figure 2.2 above is a TD Bank surveillance photo of the person withdrawing funds from the Edwards account on February 7, 2019. On that date, TD bank records show that there were two ATM withdrawals from the account totaling $700.

44. After completing the transaction, the person depicted in Figure 2.2 drove off in a vehicle bearing Massachusetts license plate 6DV279, which is registered in the name of Nosakhare Osawaru, address 49 Dana Ave., Hyde Park, Massachusetts. Nosakhare Osawaru is Esogie Osawaru's brother.

45. Victim-3 also reported that she had mailed cash via FedEx to Edward on March 19, 2019, at 49 Dana Ave., Hyde Park, Massachusetts, 02136, which is also the address listed on

Esogie's Massachusetts Driver's License, and as set forth above was used in connection with bank account openings of Howard Bhekani, Mathew Lungelo, Franklin Edward, and Milk Anthony.

D. Victim-4 from California Sends Funds to Iyalekhue's Bhekani Account.

46. On August 19, 2019, Victim-4 from Long Beach, California, filed a complaint with the FBI regarding an online consultancy work scam.

47. On or about March 5, 2020, I interviewed Victim-4 who told me she had been recruited for a job online, had a remote job interview, and believed she would be reviewing documents related to interior design. Victim-4 worked for the company for a few months but was not paid. Victim-4 located another employee (CC-4) of the company online and asked for assistance with getting paid. CC-4 told Victim-4 that he knew someone at the company and could assist.

48. CC-4 then sent Victim-4 bank checks and instructed her to deposit the checks and forward the funds from the checks via wire to bank accounts that CC-4 provided Victim-4. Victim-4 was told she had to complete this task before getting paid. Victim-4 was hesitant to deposit the checks; however, CC-4 later became aggressive in their communications, telling Victim-4 that he knew where she lived and asked Victim-4 about her child, in a manner that Victim-4 perceived as a threat.

49. Out of fear, Victim-4 complied with CC-4's request and deposited the checks and sending wires as instructed. The checks returned as invalid and Victim-4's bank account was overdrawn due to the wires. Victim-4 recalled sending two wires to Bhekani at Citizen's Bank at the direction of CC-4.

50. On or about July 26, 2019, Victim-4 sent a wire in the amount of $11,970 and on or about July 27, 2019, sent a wire in the amount of $10,370 into the Bhekani Citizens account. Between July 27, 2019 and July 31, 2019, five cash withdrawals, each under $10,000, but totaling $22,270, were made from this account at the Norwood, Roslindale and Dedham branches of Citizen's bank.

51. Figure 4.1 below is a Citizen's Bank surveillance image depicts the person purporting to be Bhekani, conducting the $2,400 cash withdrawal from Citizen's Bank in Roslindale, Massachusetts on July 29, 2019.

Fig. 4.1 Citizen's Bank Surveillance Image of July 29, 2019 Withdrawal from Bhekani Account.

The face of the person purporting to be Bhekani is not identifiable in Figure 4.1; however, the individual is wearing the same shirt worn by Iyalekhue during another Lungelo Eastern Bank transaction outlined below (depicted in Figure 6.2).

E. Victim-5 from Alabama Sends Funds to Osawaru's Edward Account.

52. On March 6, 2020, I interviewed a family member of Victim-5 who reported that Victim-5 had met a man on a romance website (CC-5) and began to send money to various people at his request. Victim-5 thought she was sending money to assist CC-5 – purportedly a US service member with whom she had been in an online relationship. Victim-5 believed the

money was a gift as well as an investment. Victim-5's family member estimated that she had sent approximately $150,000 to various people at CC-5's direction.

53. Bank records from Bank of America show that on July 19, 2018 and September 11, 2018, Victim-5 sent a $15,000 wire and a $30,000 wire to the Edward account and that each time the funds were rapidly depleted via cash withdrawals at branches in Massachusetts.

F. Victim-6 from Ohio Sends Funds to Osawaru's Anthony Account.

54. On March 6, 2020, I interviewed Victim-6 from Canton, Ohio, who reported that in February 2019, she met a man on Facebook (CC-6) who told her that he worked for the United States military and was supporting the United Nations in Syria. Victim-6 was about to have a surgery and did not have many family members or friends to help with the recovery process. CC-6 told Victim-6 that for $60,000 she could buy out his contracts with the United Nations and US military. CC-6 offered to come and take care of Victim-6. Victim-6 sent money to various people at the direction of CC-6, including to Milk Anthony.

55. Bank records for the Anthony Santander Bank account ending in 1949 show that on June 4, 2019, a $20,000 check from Victim-6 was deposited into the account. These funds were rapidly depleted via cash withdrawals at branches in Massachusetts.

56. Figure 2.4 above is a surveillance photograph from the Anthony TD Bank account ending in 9224 on March 30, 2019. A comparison of this photograph with others involved in the scheme demonstrates that the person depicted in Figure 2.4 shares the likeness of the individual depicted in Esogie Osawaru's Massachusetts Driver's License (Figure 2.1).

G. Victim-7 from Oregon Sends Money to Osawaru's Personal Bank Account.

57. According to Santander records, Osawaru maintains a personal bank account ending in 7080.

58. Victim-7 is from Newbury, Oregon and was identified in a separate FBI case as the victim of a romance scam. Victim-7 had sent money to various individuals as part of the scam.

59. On March 9, March 30, and June 10, 2020, I interviewed Victim-7 who reported that she met and developed a relationship online with a man (CC-7). Victim-7 sent money at the direction of CC-7 on several occasions, including on or about December 1, 2019 when Victim-7 mailed six separate money orders for $1,000 each to 1055 Southern Artery, Apt. 707, Quincy, Massachusetts, which also happened to be Osawaru's address at the time.

60. Two days later, on December 3, 2019, these money orders were deposited into Osawaru's personal Santander Bank account ending in 7080. These funds were depleted on December 4, 2019, via a $7,300 cash withdrawal at a Santander Bank branch in East Milton, Massachusetts. Video surveillance from Santander Bank shows that the person who made this withdrawal was Osawaru.

H. Victim-8 from New York Sends Money to Osawaru's Personal Account.

61. According to Rockland Trust bank records, Osawaru maintains a personal bank account ending in 5027.

62. On or about March 18, 2020, I interviewed Victim-8, from Jamaica, New York, who told me that she had met a man on Facebook purported named "Peter Loblock." Loblock told Victim-8 that he would be able to assist her with immigration paperwork including documents and records needed for court. Loblock required payment upfront for his assistance. On August 30, 2019, Victim-8 wired $1,280 to an account in the name Esogie Osawaru at Rockland Trust ending in 5027.

63. Bank records from Rockland Trust show that Osawaru opened an account ending in 5027 in his own name on August 28, 2019. Osawaru told the bank he was employed as a club promoter.

64. Osawaru withdrew the money Victim-8's money on September 1, 2019, via a $1,200 withdraw. Figure 5.1 is a surveillance photograph of this transaction from Rockland Trust.

Fig. 5.1 Rockland Trust Surveillance Image of Sept. 1, 2019 from Osawaru's Account.

A comparison of this photograph with others involved in the scheme demonstrates that the person depicted in Figure 5.1 shares the likeness of Esogie Osawaru's Massachusetts Driver's License (Figure 2.1).

65. The Rockland Trust Osawaru account received a $2,570 international wire on September 4, 2019, from a sender in Taiwan, and a $3,000 international wire on September 9, 2019 from a different sender in Taiwan. Osawaru withdrew these funds in cash within days following the deposits. Rockland Trust was concerned about Osawaru's banking activity and called him on September 12, 2019, to discuss the wires. Osawaru told the bank investigator that he had recently lost his job and that the wires received into his account were from family and friends. In particular as to the international wires, Osawaru told the investigator that his aunt

lived in Taiwan and was sending him money. He claimed that his aunt did not have a bank account and asked other in Taiwan people to send him the money. Based on the account activity and Osawaru's explanation for the wires, Rockland Trust closed Osawaru's account on September 12, 2019.

I. Victim-9 from Texas Sends Money to Iyalekhue's Lungelo Eastern Bank Account.

66. On February 24, 2020, I was notified by Dedham Police Department that Iyalekhue had been arrested at the Eastern Bank branch at 240 Providence Highway, Dedham, Massachusetts.

67. As noted above, on February 20, 2020, Iyalekhue had opened an account at Eastern Bank using a Liberian passport in the name of Mathew Lungelo. On the same day he opened the account, Lungelo deposited a cashier's check for $20,800, drawn off an account at BBVA USA from Victim-9. Eastern Bank was concerned about the origins of the funds and contacted a senior investigator at BBVA, the originating bank. The BBVA investigator informed Eastern Bank that their customer, an elderly woman from Scurry, Texas (Victim-9), was the victim of a scam. Eastern Bank placed the Lungelo account on hold.

68. On February 21, 2020, a person purporting to be Lungelo called Eastern Bank and inquired when the funds from the Victim-9 check would clear into his account. The Eastern Bank employee asked Lungelo if it was a local check. Lungelo told the teller it was not a local check. The Eastern Bank employee informed Lungelo the check may cleared into the account the next day on Saturday, February 22, 2020, but that it would likely be Monday, February 24, 2020, before the funds would be available in his account.

69. Iyalekhue returned to Eastern Bank on February 24, 2020, and attempted to withdraw against the fraud funds. Iyalekhue told an Eastern Bank employee that he was a

construction worker and the check from Victim-9 was for work he had completed. Eastern Bank called Dedham Police who responded to the branch.

70. When officers arrived, Iyalekhue claimed to be Mathew Lungelo. When questioned about his identity, Iyalekhue provided the date of birth listed in the Lungelo Liberian passport.

71. Initially, Iyalekhue told officers the check had arrived in his mail, and that he did not know the woman who had sent it to him. Iyalekhue stated he was unemployed and needed the money, so he deposited the check. Officers attempted to clarify this story and then Iyalekhue changed his story – stating the woman had called him and told him that if he deposited the check for her and withdrew the funds in cash, he could keep some of the funds.

72. Responding officers contacted dispatch to verify the validity of the Lungelo passport. After being informed that they were working on verifying the passport, and had concerns about his identity, Iyalekhue informed officers that his true identity was Nosayamen Iyalekhue and gave the true date of birth April 5, 1987.

73. Iyalekhue was arrested on by Dedham Police Department and charged with Obstruction of Justice for providing the false name. Figure 6.1 is a copy of Iyalekhue's booking photograph.

Fig. 6.1 Iyalekhue's booking photograph following his arrest – Feb. 24, 2020.

74. When Iyalekhue was arrested on February 24, 2020, the Dedham police officers also found credit cards in his wallet for "Gabriel Enoch." Officers asked Iyalekhue if the "Enoch" credit cards were also a false identity and Iyalekhue stated that it was a false identity.

75. According to Dedham Police Department Incident Report 2020000007787, Iyalekhue informed officers, that his white Mercedes was parked a crossed the street from Eastern Bank. Dedham Police located a white Mercedes bearing Massachusetts registration 7CK325, registered to Iyalekhue. Dedham Police subsequently sought and were granted a search warrant for this vehicle. During the search of the vehicle numerous documents in the name of Iyalekhue were discovered as well as documents in the name of Matthew Lungelo.

76. Figure 6.2 is a surveillance image taken at Eastern Bank of the person who deposited Victim-9's cashier's check for $20,800 on February 20, 2020.

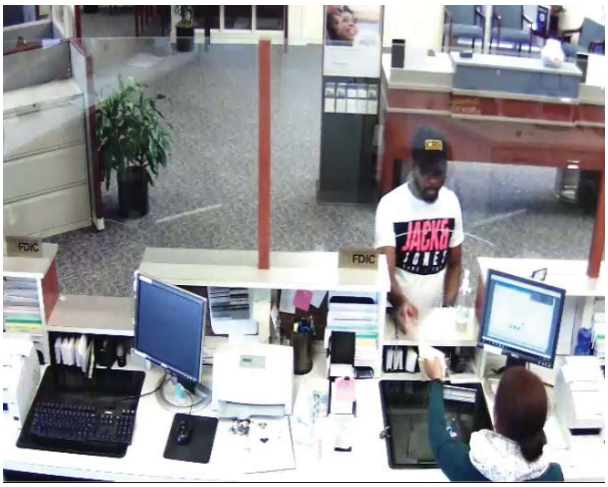

Fig. 6.2 Eastern Bank Surveillance Image of Feb. 20, 2020 depicting deposit of Victim-9's cashier's check.

A comparison of this photograph with the picture of the person who transacted on the Bhekani Citizen's Bank account on July 29, 2019 (Figure 4.1), demonstrates both individuals are wearing what appear to be the same t-shirt.

77. Victim-9 also reported that in February 2019, she had been in email contact with a man purporting to be named Charlie Clifford who expressed an interest in doing business with her. The relationship quickly transitioned from business to romantic, but Victim-9 never met Clifford.

78. At one point during their relationship, Clifford told Victim-9 that he was sending her a box that was valuable but it was stuck in customs. Victim-9 then began providing funds at Clifford's direction in an effort to pay the taxes and feels related to the box. According to Victim-9, she mailed various amount of cash to different recipients and sent a cashier's check to Mathew Lungelo at Clifford's direction

J. Additional Victims and Unemployment Insurance Fraud.

79. On or about April 10, 2020, Osawaru opened an account in his own name at the Eastern Bank branch located at 63 Franklin St, Quincy, Massachusetts.

80. On or about May 18, 2020, a check for $9,200 from Victim-10, a 76 year-old female living in Puerto Rico, was deposited in Osawaru's account at the drive-thru of Eastern Bank branch in Dedham, Massachusetts The vehicle driven during this transaction was bearing Massachusetts license plate 7JHV50, which is registered in the name of Osawaru's brother, Nosakhare Osawaru, with the address 49 Dana Ave., Hyde Park, Massachusetts.

81. Figure 7.1 is a surveillance image taken at Eastern Bank of the person who deposited Victim-10's cashier's check for $9,200 on May 18, 2020.

Fig. 7.1 Eastern Bank Surveillance Image of May 18, 2020 depicting deposit of Victim-10's cashier's check.

82. Three days later, on or about May 21, 2020, Eastern Bank's security department was notified that a stop payment had been placed on the check from Victim-10.

83. On or about May 27, 2020, I interviewed Victim-10 who told me that approximately 2 years and 4 months ago she had met a man on Facebook with whom she developed an online relationship. This individual told Victim-10 that he was in the United States Army, deployed overseas, and in financial need.

84. In early 2018, Victim-10 began sending funds to various people at this individual's direction. According to Victim-10, and my review of bank records, Victim-10 sent over $71,000 to "Franklin Edward" at the Bank of America and TD Bank accounts discussed above. Victim-10 also reported sending multiple international wires to an individual in Nigeria based upon requests from this online "friend."

85. Victim-10 also reported mailing a $9,500 check to 354 Admiral St., Providence, Rhode Island, 02908, which is a non-residential address belonging to Walgreens. Review of the tracking information from the U.S. Postal Service online tracking service reveals that the package was delivered and signed for by an "E. Osawaru" on May 15, 2020.

86. Eastern Bank records reveal that on that same day, Osawaru attempted to deposit Victim-10's check via mobile deposit. Eastern Bank representatives reported that this attempt was made from an AT&T IP address, but the deposit was unsuccessful because of the large amount of the check.

87. Osawaru's telephone service for his phone number is provided by AT&T.

88. On or about May 19, 2020, Osawaru's Eastern Bank account also received $10,710 from Washington State unemployment insurance in the name of Victim-11. Victim-11 lives in Washington State, has never applied for unemployment benefits, and reports that he has no knowledge of Osawaru.

89. On or about May 21, 2020, Osawaru's Eastern Bank received notice that an incoming credit, for a yet to be determined amount, from Pennsylvania unemployment insurance in the name of Victim-12, was incoming to Osawaru's account.

90. That same day, Osawaru returned to Eastern bank drive-thru in Dedham, MA and attempted to withdraw cash against the funds in his account. Eastern Bank, however, had placed a hold on the funds from Victims-10 and -11 and called the Dedham police.

91. Dedham police questioned Osawaru and he provided a permanent resident card indicated that he is a citizen of Nigeria. Osawaru also claimed that a few weeks ago he had deposited a check from a friend whose name he could not remember and he was at the bank to withdraw the money.

92. The Dedham police asked Osawaru if he knew the people whose unemployment payments were going into his account and he stated that he did not.

93. Dedham police then arrested Osawaru for Uttering False or Forged Records, Deeds or other Writings and Attempted Larceny over $1,200. Osawaru posted a $5,000 bond and was released later than day.

PROBABLE CAUSE THAT THE TARGET EMAIL ACCOUNT CONTAINS EVIDENCE, FRUITS, AND INSTRUMENTALITIES

94. I also have probable cause to believe that the Target Email Account (jennyrbts11@outlook.com) and associated data contains evidence, fruits, and instrumentalities of the crimes identified above.

95. As described above, Iyalekhue listed the Target Email Account as his contact email address in connection with at least 8 bank account openings. Additionally, the Target Email Account was used to register a PayPal[1] account in the name of Howard Bhekani – one of the identities Iyalekhue used to perpetrate the fraud scheme described above.

96. I learned from internet searches that the username "jennyrbts11" was used on a German dating website with a profile listing a female user living in Hannover, Germany. I located another dating profile using the "jennyrbts11" username on a Scandinavian dating website, listing a female user in Los Angeles, California. I know from my training and experience that usernames may be used in connection with a specific email address, but also more broadly as a moniker across a number of platforms.

97. Based on my training and experience, I know that banks and other online companies such as PayPal frequently communicate with customers regarding the status of their accounts via email and that such communications are sent to the email accounts listed by the customers at the time the accounts were established.

[1] PayPal is an online payments company that supports online money transfers and operates as a payment processor for online vendors, auction sites, and other commercial users. In order to register for a PayPal account, a user must provide a user name.

98. Accordingly, I believe that the Target Email Account will contain bank records, documents, and possible correspondence, and may also contain evidence of online dating, or other frauds.

99. On or about February 26, 2020, Assistant United States Attorney Sara Bloom sent Microsoft a letter requesting under 18 U.S.C. § 2703(f) that the company preserve records associated with the target account for 90 days, and on or about June 2, 2020, sent a letter renewing that request for an additional 90 days.

Technical Background

100. In addition, Microsoft allows customers to store opened incoming mail and sent mail indefinitely if they choose, subject to a maximum size limit.

101. E-mail providers also typically maintain electronic records relating to their customers. These records include account application information, account access information, and e-mail transaction information.

102. Many e-mail providers can also provide the following additional information associated with a subscriber's account: address books; buddy lists; photos, files, data, or other information; and WorldWide Web profiles or homepages.

Legal Authority

103. The government may obtain both electronic communications and subscriber information from an email provider by obtaining a search warrant. 18 U.S.C. §§ 2703(a), 2703(c)(1)(A).

104. Any court with jurisdiction over the offense under investigation may issue a search warrant under 18 U.S.C. § 2703(a), regardless of the location of the website hosting company or email provider whose information will be searched. 18 U.S.C. § 2703(b)(1)(A).

Furthermore, unlike other search warrants, § 2703 warrants do not require an officer to be present for service or execution of the search warrant. 18 U.S.C. § 2703(g).

105. If the government obtains a search warrant, there is no requirement that either the government or the provider give notice to the subscriber. 18 U.S.C. §§ 2703(b)(1)(A), 2703(c)(3).

106. This application seeks a warrant to search all responsive records and information under the control of Microsoft, a provider subject to the jurisdiction of this court, regardless of where Microsoft has chosen to store such information. Pursuant to 18 U.S.C. § 2713, the government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Microsoft's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

Request To Seal And Preclude Notice To The Subscriber(s)

107. I request that this application, the warrant, the order, and any related papers be sealed by the Court until such time as the Court pursuant to Local Rule 7.2 directs otherwise.

108. I further request that, pursuant to the preclusion-of-notice provisions of 18 U.S.C. § 2705(b), the Court order Microsoft not to notify any person (including the subscriber to whom the materials relate) of the existence of this application or the Court's Order for the earlier of one year from the date of the Court's Order or upon notice by the government within 30 days of the conclusion of its investigation, unless the Court extends such period under 18 U.S.C. § 2705(b). Non-disclosure is appropriate in this case because the Court's Order relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation,

and its disclosure may alert the targets to the existence of the investigation. There is accordingly reason to believe that notification of the existence of the Order will seriously jeopardize the investigation, including by: giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, or intimidate potential witnesses. *See* 18 U.S.C. § 2705(b). Moreover, some of the evidence in this investigation is stored electronically. If alerted to the existence of the Order, the targets could destroy that evidence, including information saved to their personal computers, on other electronic media, or in social media accounts.

Fourteen-Day Rule For Execution Of Warrant

109. Federal Rule of Criminal Procedure 41(e)(2)(A),(B) directs the United States to execute a search warrant for electronic evidence within 14 days of the warrant's issuance. If the Court issues this warrant, the United States will execute it not by entering the premises of Microsoft, as with a conventional warrant, but rather by serving a copy of the warrant on the company and awaiting its production of the requested data. This practice is approved in 18 U.S.C. § 2703(g), and it is generally a prudent one because it minimizes the government's intrusion onto Internet companies' physical premises and the resulting disruption of their business practices.

110. Based on my training and experience and that of other law enforcement, I understand that e-mail providers sometimes produce data in response to a search warrant outside the 14-day period set forth in Rule 41 for execution of a warrant. I also understand that e-mail providers sometimes produce data that was created or received after this 14-day deadline ("late-created data").

111. The United States does not ask for this extra data or participate in its production.

112. Should Microsoft produce late-created data in response to this warrant, I request permission to view all late-created data that was created by Microsoft, including subscriber, IP address, logging, and other transactional data, without further order of the Court. This information could also be obtained by grand jury subpoena or an order under 18 U.S.C. § 2703(d), neither of which contains a 14-day time limit. However, law enforcement personnel will seek to avoid reviewing any late-created data that was created by or received by the account-holder(s), such as e-mail, absent a follow-up warrant.

113. For these reasons, I request that the Court approve the procedures in Attachment B, which set forth these limitations.

CONCLUSION

114. Based on the information described above, I have probable cause to believe that

a) On or about :
   (1) October 11, 2018 (date of wire of funds from Victim 3 to the Edward TD Bank account),
   (2) November 26, 2018 (date of wire of funds from Victim 3 to the Edward TD Bank account), and
   (3) December 11, 2018 (date of wire from Victim 3 to Bhekani Santander account),

   Nosayamen Iyalekhue and Esogie Osawaru violated 18 U.S.C. § 1343 (Wire Fraud); and

b) records and data from the Target Email Account (as described in Attachment A), contain evidence, fruits, and instrumentalities of the above-listed crimes (as described in Attachment B).

115. The procedures for copying and reviewing the relevant records are set out in Attachment B.

Sworn to, under the pains and penalties of perjury, by telephone in accordance with Federal Rule of Criminal Procedure 4.1 this 11th day of June, 2020.

Michael Livingood
MICHAEL LIVINGOOD
Special Agent, Federal Bureau of Investigation

Subscribed and sworn to by telephone in accordance with Federal Rule of Criminal Procedure 4.1 this 11th day of June, 2020.

Jennifer C. Boal
Honorable Jennifer C. Boal
United States Magistrate Judge

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS